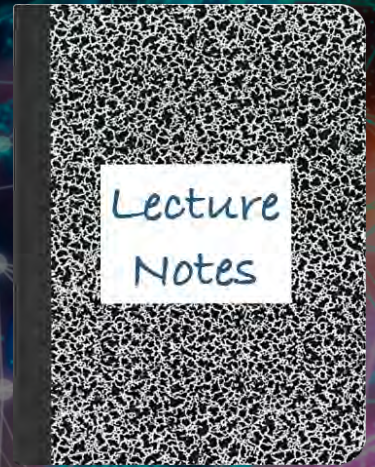


CS 419: Computer Security

Week 1: Part 4

Attacks & Motives



Paul Krzyzanowski

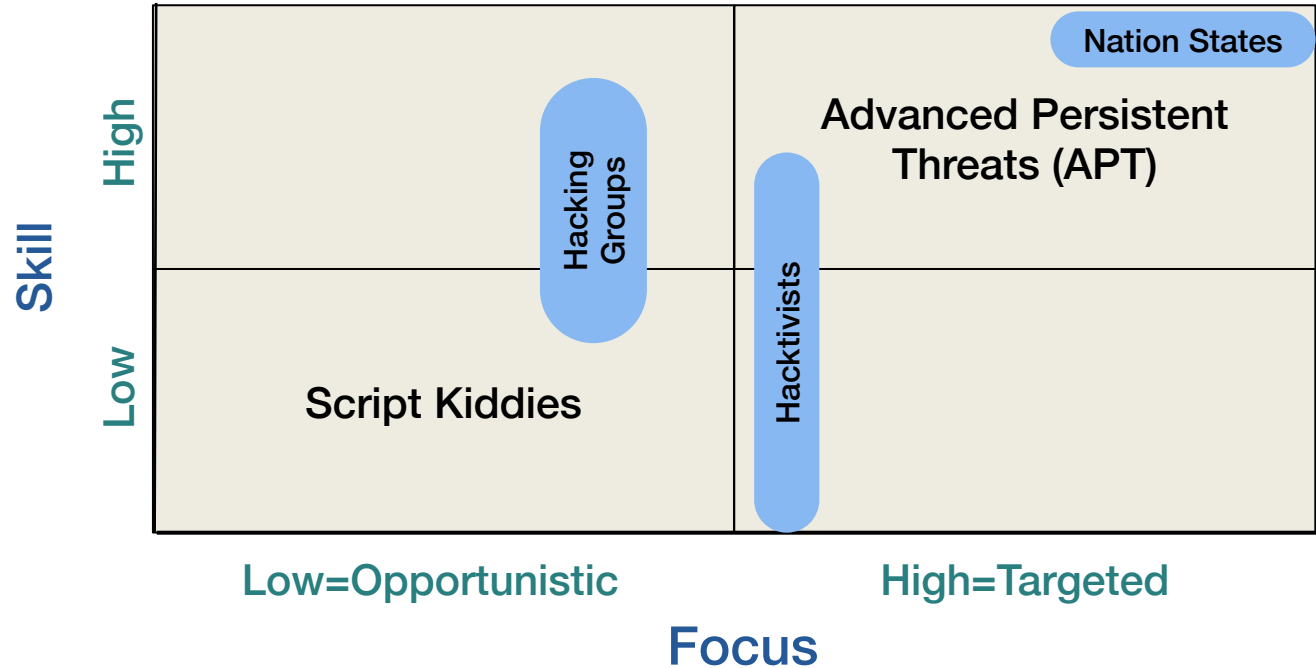
© 2022-2025 Paul Krzyzanowski. No part of this content may be reproduced or reposted in whole or in part in any manner without the permission of the copyright owner.

# The different characteristics of attackers

- **Goals**
- **Levels of access**
- **Risk tolerance**
- **Resources**
- **Expertise**
- **Economics**

# Threat Matrix

## Assess adversaries by skill vs. focus



# Script Kiddies

- **Nov 2024: Script Kiddie 'Matrix' Builds Massive Botnet** [\[link\]](#)
  - Likely Russian Hacker Exploits IoT Vulnerabilities, Many Known for Years
  - Exploits IoT device vulnerabilities such as default credentials and outdated software.
  - Heavy reliance on external scripts and existing tools
- **July 2024: New FishXProxy Phishing Kit Making Phishing Accessible to Script Kiddies** [\[link\]](#)
  - A new phishing kit, FishXProxy, makes it alarmingly easy for cybercriminals to launch deceptive attacks.
- **July 2024: Botnets are being sold on the dark web for as little as \$99** [\[link\]](#)
  - More than 20 offers for botnets for hire or sale have been discovered on dark web forums and Telegram channels this year
- **Jan 2023: ChatGPT is enabling script kiddies to write functional malware** [\[link\]](#)
- **Nov 2019: Wannabe Fraudsters Can Buy Hacking Tools on Dark Web** [\[link\]](#)
  - Prices Start as Low as a Cup of Coffee

# Teen Hacker Charged with Paralyzing Miami Schools in Embarrassingly Simple Cyberattack

GIZMODO

Alyse Stanley • September 5, 2020

A Florida teenager allegedly used an embarrassingly simple program to launch a series of DDoS attacks that helped shut down one of the nation's largest school districts for its first three days of virtual classes, the Miami Herald reported this week.

...  
“The student admitted to orchestrating eight Distributed Denial-of-Service cyberattacks, designed to overwhelm district networks,” the district said in a statement. More than 345,000 students attend public schools in Miami-Dade County, making it the fourth-largest district in the U.S.

...  
Even more embarrassing still, the student admitted that he broke the network using a decade-old, open-source tool that most bare-bones firewall software can catch, the Herald reported Saturday.

The application's called LOIC, which stands for Low Orbit Ion Cannon. Developed by 4Chan-affiliated hackers, it basically did for DDoS attacks what Microsoft Word did for word processors by streamlining the process into an easy-to-download program that even an idiot can't mess up. No hacking experience needed, just point, click, and boom! You're on your way to committing a felony. LOIC makes it easy to coordinate thousands of anonymous users to overwhelm servers by submitting tons of garbage requests en masse.

<https://gizmodo.com/teen-hacker-charged-with-paralyzing-miami-schools-in-em-1844968182>

# Launching a Ransomware Attack Against Nation Is Far Easier Than You Think

Newsweek

Naveed Jamali, Tom O'Connor, Alex J. Rouhandeh • July 8, 2021

As ransomware attacks surge to unprecedented levels, the intricacies of mounting such a potentially destructive and deceptive operation would seem to be far beyond the reach of the average netizen.

But the power to paralyze a company or a nation with malicious intent may be more readily available than is commonly thought—although it is illegal, especially for users in the United States.

A U.S. military cyberwarfare officer who spoke to Newsweek on the condition of anonymity described a very simple process for doing a great deal of damage.

"All you need is a Tor Browser and the links to the right underground markets," the officer said. "There's forums, and you can Google them."

...

It's not unlike buying a third-party smartphone application, a pre-packaged bundle of code that enables a device to perform a large range of functions with convenience. And just as consumers can download apps from leading social media companies such as Facebook, Twitter and TikTok, prospective hackers can buy the tools used by top collectives such as REvil.

<https://www.newsweek.com/launching-ransomware-attack-against-nation-far-easier-you-think-1608108>



"All the News  
That's Fit to Print"

# The New York Times

**Late Edition**

Today, overcast, breezy, chilly, rain, high 56. Tonight, cloudy, a bit of rain, low 52. Tomorrow, early showers, then some sunshine, warmer, high 67. Weather map is on Page 26.

VOL. CLXX ... No. 59,074

© 2021 The New York Times Company

NEW YORK, SUNDAY, MAY 30, 2021

\$6.00

## *From Russians, Ransomware, Made to Order*

*This article is by Andrew E. Kramer, Michael Schwirtz and Anton Troianovski.*

MOSCOW — Just weeks before the ransomware gang known as DarkSide attacked a major American pipeline, disrupting gasoline and jet fuel deliveries up and down the East Coast of the United States, the group was turning the

screws on a small, family-owned publisher based in the American Midwest.

Working with a hacker who went by the name of Woris, DarkSide launched a series of attacks meant to shut down the websites of the publisher, which works mainly with clients in primary school education, if it refused to meet a \$1.75 million ransom demand. It even threatened to contact the company's clients to falsely warn them that it had obtained information the gang said could be used by pedophiles to make fake identification cards that would allow them to enter schools.

Woris thought this last ploy was a particularly nice touch.

"I laughed to the depth of my soul about the leaked IDs possibly being used by pedophiles to enter the school," he said in Russian in a secret chat with DarkSide obtained by The New York Times. "I didn't think it would scare them that much."

DarkSide's attack on the pipeline owner, Georgia-based Colonial Pipeline, did not just thrust the gang onto the international stage. It also cast a spotlight on a rapidly expanding criminal industry based primarily in Russia that has morphed from a specialty demanding highly sophisticated hacking skills into a conveyor-belt-like process. Now, even

*Continued on Page 14*

# Who are the adversaries?

- **Hackers**

- Good or evil
  - **White hat hackers:** do not intend to cause damage; goal = profit or fixing bugs
  - **Black hat hackers:** profit by hacking or selling services to the highest bidder
- Test boundaries of the system – get to know the system better than designers
- Only a small % are smart
- Bug hunters – find vulnerabilities
- Exploit writers – write code to exploit the vulnerabilities

- **Criminals**

- Individuals or small groups
- Don't necessarily reap huge \$ but are often creative



# Who are the adversaries?

- **Malicious insiders**

- Insidious because they are indistinguishable from legitimate, trusted insiders
- Perimeter defenses don't work
- Often have high levels of access

- **Industrial spies**

- Product designs, trade secrets, project bids, finances, employee info
- Can hire/bribe employees to reveal trade secrets or become inside attackers
- ... or resort to dumpster diving
- **Risk-averse**: reputation of company (or country) damaged if caught

# Who are the adversaries?

- **Press (& politicians)**

- Social engineering, bribing, dumpster diving, track movements, eavesdrop, break in
- Also generally risk averse for fear of losing one's reputation & career

- **Organized crime**

- More opportunities to make or launder money!
- Money laundering is easier with EFT and cryptocurrency

- **Police**

- Risk averse but have law on their side (e.g., search warrants, seizing evidence)
- Not above breaking law: wiretaps, destruction of evidence, disabling body cameras, illegal search & seizure

# Organized Crime

## Example: Russian Business Network (RBN)

- **Operates on numerous ISPs worldwide**
- **Internet service provider run by criminals for criminals**
  - Host platform for illegal businesses
- **Domains registered to anonymous addresses**
  - Does not advertise
  - Trades in untraceable electronic transactions
- **Known for delivering fake anti-spyware & anti-malware software**
  - Used for PC hijacking and personal identity theft
- **One of the world's worst spammer, malware, and phishing networks**

# Who are the adversaries?

- **Hactivists, Terrorists (freedom fighters)**

- Motivated by geopolitics, religion, or a set of ethics
- Examples:
  - **Anonymous Sudan** – targets anti-Muslim activities but may be Russian-backed
  - **Cyber Partisans** – Belarusian hactivists against the Belarusian government
  - **DCLeaks** – claims to be Americans concerned with freedom of speech but at least some individuals were Russian
  - **Decocidio** – an autonomous hacking group part of Earth First, a radical environmental protest group
  - **Honker Union** – group in China mostly attacking U.S. websites
  - **Garnesia\_Team**, Moroccan Black Cyber Army – pro-Palestinian attacks
  - **Ukrainian Cyber Alliance** – Ukrainian hackers fighting Russia
- Usually more concerned with causing harm than getting specific information
- Usually (but not always) low budgets & low skill levels
- Have grown more sophisticated lately
  - *IT Army of Ukraine* vs. Russia's *KillNet* group



# Hacktivist Group Leaks Disney's Slack Channels Over its Stance on AI Images

Matt Growcoat • July 17, 2024

A group of hackers has leaked over a terabyte of data from Disney's internal communications platform over the company's stance on AI imagery.

The group called NullBulge released the data from Disney's Slack channels yesterday through a peer-to-peer network. It says it is motivated to "protect artists' rights and ensure fair compensation for their work".

That is different from a hacker's usual modus operandi who often demand ransoms. NullBulge leaked the dossier of photos, conversations, and unreleased projects quite quickly saying that making demands from Disney would be futile.

<https://petapixel.com/2024/07/17/hacktivist-group-leaks-disneys-slack-channels-over-its-stance-on-ai-images/>



# Who are the adversaries?

- **National intelligence organizations**

- Huge money & long-term goals
- Somewhat risk averse
  - Bad public relations
  - Do not want leaks to reveal attack techniques
- Often have a lot of influence
  - NSA was instrumental in the adoption of 56-bit keys for DES or the Dual\_EC\_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator)
  - Lenovo computers, owned partially by the Chinese government's Academy of Sciences has been accused of “malicious circuits” built into the computers
  - NSA planted backdoors into Cisco routers built for export that allows the NSA to intercept any communications through those routers.

- **Nation-states: Infowarriors, cyber warfare**

- Huge money & short-term goals
- Disrupt power grids, commerce, transportation
- EMP weapons, spread selective information, misinformation, blackmail

# Naming Schemes for APT Groups

## Names usually come from organizations that identify the attacker

- There is no standard naming convention

### 1. APT Numbering

Coined by Mandiant (now part of FireEye)

- Sequential numbers in order of discovery
  - APT1 – attributed to the 2<sup>nd</sup> Bureau of China's People's Liberation Army – Unit 6139
  - APT29 – attributed to Russia's Foreign Intelligence Service

### 2. Animal Themes

Used by CrowdStrike

- **Panda:** Chinese APTs (Deep Panda, Gothic Panda, ...)
- **Bear:** Russian APTs (Cozy Bear, Fancy Bear, ...)
- **Kitten:** Iranian APTs (Charming Kitten)
- **Tiger:** Indian APTs (Patchwork Tiger)

# Naming Schemes for APT Groups

## 3. Numeric Codes

Used by FireEye, Palo Alto Networks

- E.g., *Group-3390*, *UNC2452*
- Tracked until more details are confirmed about their origin

## 4. Threat Actor Names

Named after campaigns or characteristics

- **Lazarus Group**: North Korean group infamous for the Sony Pictures hack
- **Equation Group**: allegedly linked to the NSA

## 5. Microsoft Naming Scheme

Two-word combination of

*Weather* – identifies geography

*Adjective* or *noun*: identifies the group

- Weather Terms
  - **Typhoon**: China
  - **Cyclone**: Iran
  - **Blizzard**: Russia
  - **Sleet**: North Korea
  - **Sandstorm**: Middle East
  - **Tempest**: Financially-motivated groups
  - **Storm**: Unconfirmed threat group
- E.g., Salt Typhoon, Midnight Blizzard

# Cyber Warfare: Nation State Attacks

# 2024 Highlights: State-Sponsored Espionage (1)

- 1. Salt Typhoon Campaign** (Year-long)  
Chinese actors targeted telecoms globally, compromising surveillance systems and wiretap platforms
- 2. Microsoft Email Breach** (January)  
Russian state-sponsored group Midnight Blizzard breached Microsoft's corporate emails, targeting leadership and legal teams for espionage.
- 3. Pro-Palestinian Internet Archive Attack** (October)  
SN\_BlackMeta launched a DDoS attack and stole user data for 33M from the Internet Archive
- 4. Iran's Hack of Trump Campaign** (August)  
The breach was attributed to Iranian actors who exposed campaign documents



# 2024 Highlights: State-Sponsored Espionage (2)

- 1. North Korean IT Worker Espionage (May–July)**  
North Korean agents infiltrated U.S. job markets, including an email security firm, to deploy malware and fund nuclear programs.
- 2. Iran's Hack of Trump Campaign (August)**  
Breach attributed to Iranian actors, exposing campaign documents.
- 3. Chinese Telecom Breaches (November)**  
U.S. telecoms compromised, leaking call records and surveillance information.

# A Growing Army of Hackers Helps Keep **Bloomberg** Kim Jong Un in Power

North Korea relies on cybercrime to fund its nuclear arms program and prop up the ailing economy.

[Jon Herskovitz & Jeong-Ho Lee](#) • December 21, 2021

Kim Jong Un marked a decade as supreme leader of North Korea in December. Whether he can hold on to power for another 10 years may depend on state hackers, whose cybercrimes finance his nuclear arms program and prop up the economy.

According to the U.S. Cybersecurity & Infrastructure Security Agency, North Korea's state-backed "malicious cyberactivities" target banks around the world, steal defense secrets, extort money through ransomware, hijack digitally mined currency, and launder ill-gotten gains through cryptocurrency exchanges. Kim's regime has already taken in as much as \$2.3 billion through cybercrimes and is geared to rake in even more, U.S. and United Nations investigators have said.

The cybercrimes have provided a lifeline for the struggling North Korean economy, which has been hobbled by sanctions. Kim has shown little interest in returning to negotiations that could lead to a lifting of sanctions if North Korea winds down its nuclear arms program.

Money from cybercrimes represents about 8% of North Korea's estimated economy in 2020, which is smaller than when Kim took power, according to the Bank of Korea in Seoul.

<https://www.bloomberg.com/news/articles/2021-12-21/north-korean-army-of-cybercriminals-props-up-kim-s-nuclear-program-and-economy>

# Stuxnet – 2010, U.S. & Israel (?)

- **Targeted centrifuges used to purify uranium in Iran**
- **Attacked Siemens centrifuges via a SCADA interface**
  - Phase 1
    - Possible initial installation via thumb drive
    - **Air gapped systems** – systems physically separated from other networks
    - Propagated across Microsoft Windows Systems
    - Searched for systems running Siemens Step7 control software
  - Phase 2
    - Altered the spin of the centrifuges while making it look like everything was fine
- **Showed that cyber attacks can cause real-world damage**
- **Pipelines, electric grids, banking, ... are at risk**

# Hackers Bring Down Government Sites in Ukraine

A cyberattack defaced the Foreign Ministry website with a message saying “Be afraid,” a day after the latest round of talks between Moscow and the West aimed at forestalling a Russian invasion.

Andrew Kramer • January 14, 2022

KYIV, Ukraine — Hackers brought down several Ukrainian government websites on Friday, posting a message on the site of the Foreign Ministry saying, “Be afraid and expect the worst.” It was the latest in a long line of cyberattacks targeting the country amid its conflict with Russia.

The attack on Friday was ominous for its timing, coming a day after the apparent breakdown of diplomatic talks between Russia and the West intended to forestall a threatened Russian invasion of Ukraine. The message appeared in Ukrainian, Russian and Polish on the foreign ministry website.

“As a result of a massive cyber attack, the websites of the Ministry of Foreign Affairs and a number of other government agencies are temporarily down,” the ministry said in a statement.

Diplomats and analysts have been anticipating a cyberattack on Ukraine, but proving such actions is notoriously difficult. Ukraine did not directly blame Russia for the attack, but pointedly noted that there was a long record of Russian online assaults against Ukraine.

<https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html>

# Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says

FBI

Partnerships, joint operations, and private sector vigilance can help us fight back

April 18, 2024

FBI Director Christopher Wray on April 18 warned national security and intelligence experts, as well as students, that risks the government of China poses to U.S. national and economic security are “upon us now”—and that U.S. critical infrastructure is a prime target.

...

But the CCP also wants to prevent the United States from being able to get in the way of a potential future “crisis between China and Taiwan by 2027,” he said. Americans are starting to feel the effects of this sprint, he said, pointing to “cyber intrusions and criminal activity” as early deterrence efforts by the CCP.

...

Similarly, he said, during the FBI’s recent Volt Typhoon investigation, the Bureau found that the Chinese government had gained illicit access to networks within America’s “critical telecommunications, energy, water, and other infrastructure sectors.” But, he noted, the CCP has also targeted critical infrastructure organizations through more “scattershot, indiscriminate cyber campaigns” that also impact other victims—such as their Microsoft Exchange hack in 2021, which “targeted networks across a wide range of sectors.”

<https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says>



# Chinese hack of US telecoms compromised more firms than previously known, WSJ says



Reuters • January 5, 2025

WASHINGTON, Jan 5 (Reuters) - A Chinese hack compromised even more U.S. telecoms than previously known, including Charter Communications, Consolidated Communications and Windstream, the Wall Street Journal reported late on Saturday, citing people familiar with the matter.

Hackers also exploited unpatched network devices from security vendor Fortinet and compromised large network routers from Cisco Systems, the newspaper reported.

In addition to deep intrusions into AT&T and Verizon (VZ.N, hackers pierced other networks belonging to Lumen Technologies and T-Mobile, according to the report.

China denied engaging in such actions and accused the United States of peddling disinformation.

<https://www.reuters.com/business/media-telecom/chinese-hack-us-telecoms-compromised-more-firms-than-previously-known-wsj-says-2025-01-05/>

# More than half of foreign cyberattacks against China in 2019 originated in the US, China report says

China recently tightened its cybersecurity rules, requiring “critical information infrastructure” to undergo a more rigorous review process

Coco Feng • August 12, 2020

More than half of computer malware attacks in China from overseas entities in 2019 originated in the US, according to data from a government-affiliated cybersecurity team.

The total amount of computer malware attacks captured by the National Computer Network Emergency Response Technical Team (CNCERT) was over 62 million in 2019, and around 53.5 per cent of foreign attacks were from the US, lower than a year before when there were in excess of 100 million incidents, the Team said.

Russia and Canada were the second and third largest contributors to computer malware attacks against China, accounting for 2.9 and 2.6 per cent respectively of the total number of foreign attacks.

The number of new malicious attacks directed against mobile networks was nearly 2.8 million in 2019, 1.4 per cent lower than a year earlier, the first decline in such attacks in five years, according to CNCERT.

<https://www.scmp.com/tech/policy/article/3097070/more-half-foreign-cyberattacks-against-china-2019-originated-us-china>

# U.S. Escalates Online Attacks on Russia's Power Grid

The New York Times

By David E. Sanger and Nicole Perloth • June 15, 2019

The United States is stepping up digital incursions into Russia's electric power grid in a warning to President Vladimir V. Putin and a demonstration of how the Trump administration is using new authorities to deploy cyber tools more aggressively, current and former government officials said.

In interviews over the past three months, the officials described the previously unreported deployment of American computer code inside Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections.

Advocates of the more aggressive strategy said it was long overdue, after years of public warnings from the Department of Homeland Security and the F.B.I. that Russia has inserted malware that could sabotage American power plants, oil and gas pipelines, or water supplies in any future conflict with the United States.

<https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>

# Are our intelligence efforts secure?

**Government agencies try to develop – and pay for –  
the best attacking & defense techniques**

**But...**

# The American Military Sucks at Cybersecurity

A new report from US military watchdogs outlines hundreds of cybersecurity vulnerabilities.

Matthew Gault • January 23, 2019

The Department of Defense is terrible at cybersecurity. That's the assessment of the Pentagon's Inspector General (IG), who did a deep dive into the American military's ability to keep its cyber shit on lockdown. The results aren't great. "As of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008," the Inspector General said in a new report.



The new report is a summary of the IG's investigations into Pentagon cybersecurity over the previous year. It looked at 20 unclassified and four classified reports that detailed problems with cybersecurity and followed up to see if they'd been addressed. Previously, the IG had recommended the Pentagon take 159 different steps to improve security. It only took 19 of them.

[https://motherboard.vice.com/en\\_us/article/7xy5ky/the-american-military-sucks-at-cybersecurity](https://motherboard.vice.com/en_us/article/7xy5ky/the-american-military-sucks-at-cybersecurity)



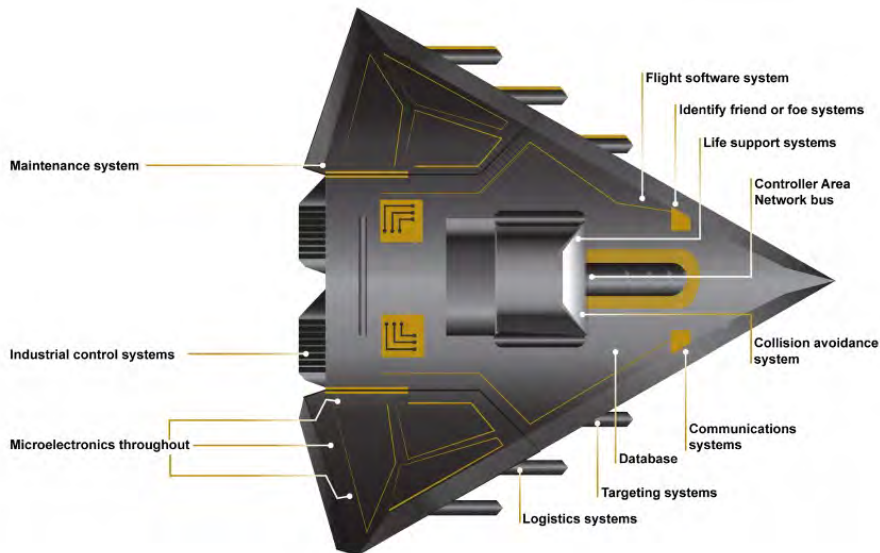
# US Advanced Weaponry Is Easy to Hack, Even by Low-Skilled Attackers

By Ionut Ilaşcu • October 9, 2018

Major weapon systems developed by the US Department of Defense are riddled with vulnerabilities that make them an easy target for adversaries trying to control them or disrupt their functions.

As the DoD plans to spend about \$1.66 trillion to advance its weapons arsenal, the US Government of Accountability Office (GAO) finds reports from various development stages of the systems showing that mission-critical vulnerabilities are a regular find in "nearly all weapon systems that were under development."

Testing teams charged with probing the resilience to cyber attacks were able to take control or disable the target using basic tools and techniques. Sometimes, just scanning the system caused parts of it to shut down.



## March 2017 – Wikileaks publishes CIA Vault 7

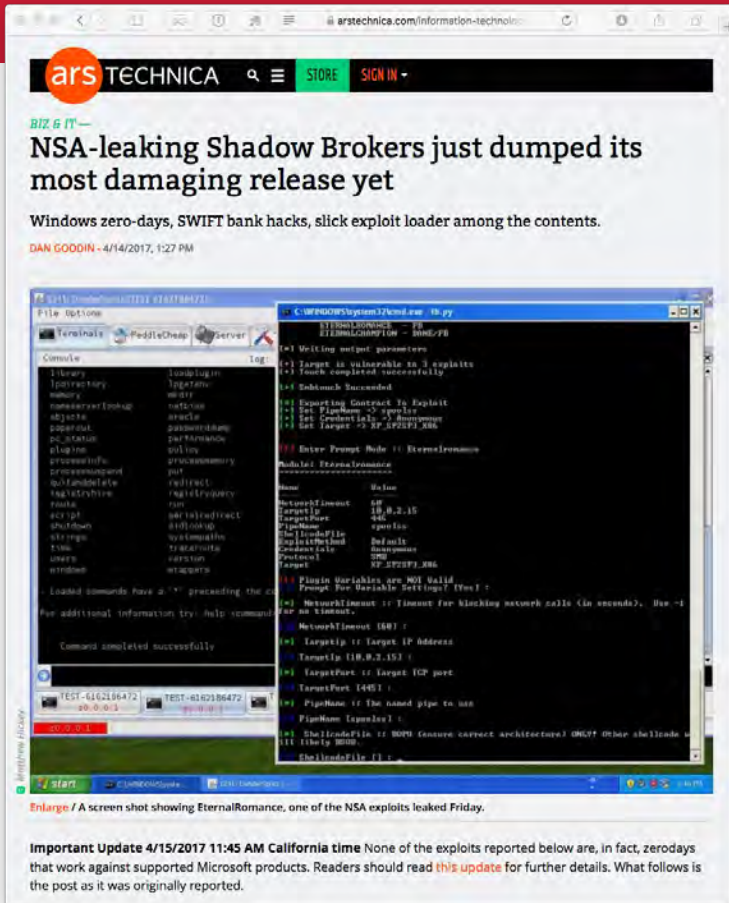
- **8,761 documents stolen from the CIA**
- **Document spying operations & hacking tools**
- **iOS and Android vulnerabilities**
- **Bugs in Windows**
- **Ability to turn some smart TVs into listening devices**

# April 2017 – Theft from the NSA

## Shadow Brokers

Group that leaked a gigabyte of the National Security Agency's weaponized software exploits over an eight-month period

**Most vulnerabilities were patched  
... but lots of systems never get updated**



The screenshot shows a web browser displaying an article from Ars Technica. The article title is "NSA-leaking Shadow Brokers just dumped its most damaging release yet". Below the title is a sub-headline: "Windows zero-days, SWIFT bank hacks, slick exploit loader among the contents." The author is identified as "DAN GOODIN" and the date is "4/14/2017, 1:27 PM". The main content of the article is a screenshot of a Windows command prompt window. The command prompt shows the execution of the "EternalRomance" exploit. The output of the exploit is displayed in a separate window, showing the following details:

```
Module: EternalRomance
-----
Name      Date
-----
NetworkIn  1P
TargetIP  192.2.15
TargetPort 445
PipeName  specific
Shellcode  default
CommandLine  CMD
Protocol  XP_SP2SP3_X86
Target

! Plugin Variables are NOT valid
! Prompt for Variable Settings? (Y/N) :
! NetworkIn :: Timeout for blocking network calls (in seconds). 0 = 1
! For no timeout.
! NetworkIn (IP) :
! TargetIP :: Target IP Address
! TargetIP 192.2.153 :
! TargetPort :: Target TCP port
! TargetPort (445) :
! PipeName (specific) :
! ShellcodeFile :: Worm (ensure correct architecture) (MSFP) Other shellcode s
!!! libely none
! ShellcodeFile (I) :
```

Below the screenshot, there is a caption: "Enlarge / A screen shot showing EternalRomance, one of the NSA exploits leaked Friday." At the bottom of the article, there is an "Important Update" section dated "4/15/2017 11:45 AM California time", stating that none of the exploits reported are zero-days that work against supported Microsoft products and directing readers to read a linked update for further details.

# Sept 2017 – TAO tools theft from NSA

- Former NSA contractor stole >50 TB of highly sensitive data
- Includes 75% of hacking tools belonging to NSA's Tailored Access Operations
- *"took NSA materials home so that he could become better at his job"*
- *"Theft came to light during the investigation of a series of NSA-developed exploits that were mysteriously published online by a group calling itself Shadow Brokers."*



The screenshot shows a web browser displaying an article on the Ars Technica website. The URL in the address bar is 'ars Technica.com/tech-policy/2017/02/'. The page header includes the 'ars TECHNICA' logo, a search icon, and links for 'STORE' and 'SIGN IN'. The article title is 'Former NSA contractor may have stolen 75% of TAO's elite hacking tools'. Below the title, it states 'Prosecutors reportedly plan to charge Harold T. Martin with espionage.' and is dated 'DAN GOODIN - 2/8/2017, 8:05 PM'. The main text begins with 'On Monday, The Washington Post reported one of the most stunning breaches of security ever. A former NSA contractor, the paper said, stole more than 50 terabytes of highly sensitive data. According to one source, that includes more than 75 percent of the hacking tools belonging to the Tailored Access Operations. TAO is an elite hacking unit that develops and deploys some of the world's most sophisticated software exploits.' There are two 'FURTHER READING' sections with blue icons. The first one is titled 'Confirmed: hacking tool leak came from "omnipotent" NSA-tied group' and the second is 'NSA-linking Shadow Brokers lob Molotov cocktail before exiting world stage'. At the bottom, it says 'Listing image by National Security Agency'.

# Attack Motives

# Attack Motives: Criminal attacks

- **Fraud**
- **Theft (financial)**
  - Hacking, extortion (ransomware), scams (pyramid schemes, fake auctions, ...)
- **Extortion**
- **Scams**
  - Pay \$\$ and get little or nothing back: pyramid schemes, fake auctions
- **Destruction**

# Attack Motives: Privacy violations

- **Intellectual property theft**

- Challenge: sometimes we want to make data (e.g., software, music, movies, photos, books) accessible but keep control of its distribution

- **Identity theft**

- **Surveillance**

- Databases
- Installation of surveillance software
- Traffic analysis
- Large-scale surveillance
  - E.g., U.S. NSA's ECHELON, China Skynet

# Profit



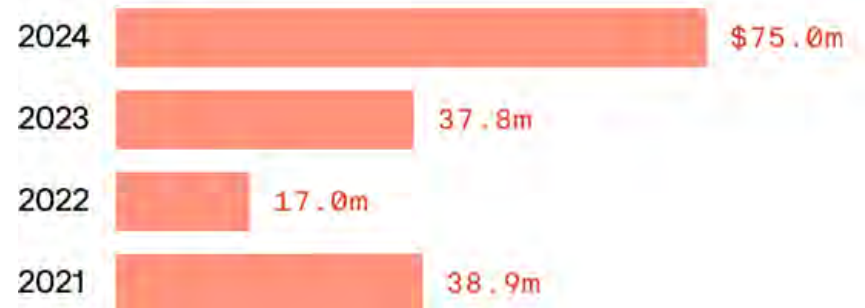
# Ransomware can be highly profitable

## Ransomware allows direct monetization of attacks

- **2023**
  - Median price paid to attackers: \$200,000
  - Highest price: \$37.8 million
- **2024**
  - Median price paid to attackers: \$1,500,000
  - Highest price: \$75 million

## Largest ransom payments made to hackers from 2021-2024

As of July 2024



Data: Chainalysis; Note: 2024 record as of July; Chart: Axios Visuals

# Some ransomware attacks

- **CDK Global (serving car dealerships) – June 2024 – crippled car sales – \$25M**
- **Colonial Pipeline – May 2021 – Stopped fuel delivery – \$4.4M**
- **Costa Rican govt – April 2022 – shut down multiple govt systems - \$30M/day**
- **JBS Meats – May 2021 – Stopped meat delivery – \$11M**
- **Kronos – December 2021 – workforce mgmt software affected numerous companies**
- **Maersk – June 2017 – shipping company suffered ~\$300M in losses – 2 weeks to recover**
- **Acer – March 2021 – demanded \$50M**
- **Brenntag – chemical distribution – \$4.4M**
- **Kaseya – IT monitoring – 800-1500 businesses – demanded \$70M**
- **Quanta – contract manufacturing (Apple) – demanded \$50M**

# Attack Motives: Finding vulnerabilities is a business

- **Dozens of companies have bug bounty programs**
  - They'll pay you if you find security vulnerabilities or come up with exploits
- **Some companies specialize in acquiring exploits**
  - And sell them to institutions, including government agencies



The screenshot shows the Zerodium website. At the top left is the Zerodium logo. Below it, the text reads "Our Exploit Acquisition Program". Further down, there is a section titled "Program Overview". The main body of text states: "ZERODIUM is the world's leading exploit acquisition platform for... capabilities. We pay BIG bounties to security researchers to acquire... research. While the majority of existing bug bounty programs accept... very low rewards, at ZERODIUM we focus on high-risk vulnerabilities... highest rewards (up to \$2,500,000 per submission)." The background is white with blue and purple accents.

The Washington Post

## The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities

Brian Fung • August 31, 2013

<https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/>

## The Hacker News

### Apple will now pay hackers up to \$1 million for reporting vulnerabilities

August 09, 2019 Mohit Kumar



...es of its bug bounty program by announcing a few major changes  
Black Hat security conference yesterday.

# Apple pays record \$100,500 to student who found Mac webcam hack



William Gallagher • January 25, 2022

A cyber security student has shown Apple how hacking its Mac webcams can then also leave devices fully open to hackers, earning him \$100,500 from the company's bug bounty program.

Ryan Pickren, who previously discovered an iPhone and Mac camera vulnerability, has been awarded what is believed to be Apple's largest bug bounty payout.

According to Pickren, the new webcam vulnerability concerned a series of issue with Safari and iCloud that he says Apple has now fixed. Before it was patched, a malicious website could launch an attack using these flaws.

In his [full account of the exploit](#), Pickren explains it would give the attacker full access to all web-based accounts, from iCloud to PayPal, plus permission to use the microphone, camera, and screensharing. If the camera were used, however, its regular green light would still come on as normal.

[https://appleinsider.com/articles/22/01/25/apple-pays-record-100500-to-student-who-found-mac-webcam-hack?utm\\_medium=rss](https://appleinsider.com/articles/22/01/25/apple-pays-record-100500-to-student-who-found-mac-webcam-hack?utm_medium=rss)

# Blockchain bridge Wormhole pays record \$10m bug bounty reward

Adam Bannister • May 23, 2022

An ethical hacker has earned a record \$10 million bug bounty reward after discovering a critical security vulnerability in the Wormhole core bridge contract on Ethereum.

Wormhole is a decentralized, universal message-passing protocol that enables interoperability between blockchains such as Ethereum, Terra, and Binance Smart Chain (BSC).

## Held to ransom

An attacker exploiting the vulnerability “could have held the entire protocol [to] ransom with the threat that the Ethereum Wormhole bridge would be bricked, and all the funds residing in that contract lost forever”, according to a proof of concept (PoC) posted to GitHub by Immunefi.

The PoC also noted that “\$736 million worth of assets [were] residing in the contract at the time of submission”.

# Hackers get \$886,250 for 49 zero-days at Pwn2Own Automotive 2025

Sergiu Gatlan • January 24, 2025

The Pwn2Own Automotive 2025 hacking contest has ended with security researchers collecting \$886,250 after exploiting 49 zero-days.

- The Synacktiv team used a single integer overflow to exploit the Sony IVI.
- The Synacktiv team used a single buffer overflow to exploit the Autel MaxiCharger.
- Thanh Do of Team Confused was able to confuse the Alpine iLX-507 with a single stack buffer overflow.
- The PHP Hooligans used a single OS command injection bug to exploit the Kenwood DMX958XR.
- Sina Kheirkhah of Summoning Team used a command injection bug on the Alpine iLX-507.
- Evan Grant used an OS command injection bug to exploit the Kenwood DMX958XR.

<https://www.bleepingcomputer.com/news/security/hackers-get-886-250-for-49-zero-days-at-pwn2own-automotive-2025/>

<https://www.zerodayinitiative.com/blog/2025/1/23/pwn2own-automotive-2025-day-three-and-final-results>

# Paying for exploits – supply & demand

## Price of zero-day exploits rises as companies harden products against hackers



A startup is now offering millions of dollars for tools to hack iPhones, Android devices, WhatsApp, and iMessage

April 6, 2024

Tools that allow government hackers to break into iPhones and Android phones, popular software like the Chrome and Safari browsers, and chat apps like WhatsApp and iMessage, are now worth millions of dollars — and their price has multiplied in the last few years as these products get harder to hack.

On Monday, startup Crowdfense published its updated price list for these hacking tools, which are commonly known as “zero-days” because they rely on unpatched vulnerabilities in software that are unknown to the makers of that software.

Companies like Crowdfense and one of its competitors, Zerodium, claim to acquire these zero-days with the goal of reselling them to other organizations, usually government agencies or government contractors, which claim they need the hacking tools to track or spy on criminals.

# Attack Motives: Finding exploits is a career

The image is a screenshot of the ScienceSoft website's 'Penetration Testing Services' page. The website has a blue and white color scheme. At the top left is the ScienceSoft logo with the tagline 'PROFESSIONAL SOFTWARE DEVELOPMENT'. The top navigation bar includes links for 'ABOUT', 'SERVICES', 'INDUSTRIES', 'CASE STUDIES', 'BLOG', and a 'LET'S TALK' button. A search icon is located in the top right corner. Below the navigation, a breadcrumb trail reads 'Home > Cybersecurity > Security Testing > Penetration Testing'. The main heading is 'Penetration Testing Services'. To the left of the main content is a sidebar menu with categories: 'Cybersecurity Consulting', 'Security Testing', 'Vulnerability Assessment', 'Penetration Testing' (highlighted), 'Case Studies', 'Special Offer: Remote Work Security Assessment', 'SIEM', 'IBM Security QRadar', 'QLEAN for QRadar health check', and 'QWAD WinCollect Assisted Deployment'. The main content area features a large, colorful illustration of a cybersecurity ecosystem. It includes server racks labeled 'PHYSICAL SECURITY', 'REMOTE ACCESS', and 'CLOUD SERVICES'. A central green shield with a padlock represents security. To the right, there are icons for 'CLIENT-SIDE SECURITY', 'WEB APPLICATION SECURITY', and 'MOBILE APPLICATION SECURITY'. A magnifying glass icon is positioned over the left side of the illustration, symbolizing the focus on finding vulnerabilities.

**ScienceSoft**  
PROFESSIONAL SOFTWARE DEVELOPMENT

ABOUT SERVICES INDUSTRIES CASE STUDIES BLOG LET'S TALK

CYBERSECURITY

Home > Cybersecurity > Security Testing > Penetration Testing

## Penetration Testing Services

Cybersecurity Consulting

Security Testing

Vulnerability Assessment

**Penetration Testing**

Case Studies

Special Offer: Remote Work Security Assessment

SIEM

IBM Security QRadar

QLEAN for QRadar health check

QWAD WinCollect Assisted Deployment

PHYSICAL SECURITY

REMOTE ACCESS

CLOUD SERVICES

CLIENT-SIDE SECURITY

WEB APPLICATION SECURITY

MOBILE APPLICATION SECURITY



# Attack Motives: Building exploits is a career



The screenshot shows the CIA website's 'Careers & Internships' page. At the top left is the CIA logo and the text 'CENTRAL INTELLIGENCE AGENCY'. To the right is the slogan 'THE WORK OF A NATION. THE CENTER OF INTELLIGENCE.' and a search bar for 'CIA.gov...'. Below the header is a navigation menu with links for HOME, ABOUT CIA, CAREERS & INTERNSHIPS, OFFICES OF CIA, NEWS & INFORMATION, LIBRARY, and KIDS' ZONE. The main content area is titled 'Careers & Internships' and features a banner image of a diverse group of people. On the left side, there is a sidebar with 'Search Jobs' and 'Browse Jobs by Category'. The main content area displays a job listing for 'Cyber Exploitation Officer' with details on work schedule, salary, and location.

**Careers & Internships**

Home » Careers & Internships » Search Jobs » Business » Cyber Exploitation Officer

**Cyber Exploitation Officer**

**Work Schedule:** Full Time  
**Salary:** \$58,638 - \$103,639\*  
**Location:** Washington, DC metropolitan area

\*Higher starting salary possible depending on experience



The screenshot shows the NSA website's 'CYBER CAREERS' page. At the top is the NSA logo and the slogan 'Where Intelligence Goes to Work®'. Below the header is a navigation menu with links for NSA Home, Careers, Virtual Recruitment, Benefits, Life At NSA, Programs, Career Development, Student Portal, Applicant Portal, Diversity, Featured Schools, FAQ, Resources, and NSA.gov. The main content area is titled 'CYBER CAREERS' and features a large banner image of a city at night. The text describes the NSA's need for cyber professionals to protect and defend U.S. government IT systems and to exploit the intelligence of adversaries. It also mentions the agency's tradition of excellence and the skills needed for a career at NSA.

**NSA National Security Agency**  
*Where Intelligence Goes to Work®*

NSA Home | Careers | Virtual Recruitment | Benefits | Life At NSA | Programs | Career Development | Student Portal | Applicant Portal | Diversity | Featured Schools | FAQ | Resources | NSA.gov

## CYBER CAREERS

The National Security Agency employs a wide variety of cyber professionals to help protect and defend U.S. government IT systems, and to help exploit the intelligence of adversaries.

As our use of technologies grows exponentially, so do our country's vulnerabilities. Our national security depends on the stability and reliability of our communications infrastructure. The cyber threat to IT and national security systems has never been greater.

As a cyber professional at NSA, you will become a part of a tradition of excellence, poised to lead the nation in the protection of our country's national interests in cyberspace for years to come.







**The Skills We Need**

If you have a background in any of the following fields, consider a cyber career at NSA.

# Attack Motives: Privacy violations

## Surveillance

- Databases
- Installation of surveillance software
- Traffic analysis
- Large-scale surveillance
  - E.g., ECHELON, Skynet

<   **Bloomberg Businessweek**    


Technology

■ January 29, 2024, 4:00 AM EST

### There's So Much Data Even Spies Are Struggling to Find Secrets

● Scouring open-source intelligence may not have the same cachet as undercover work, but it's become a new priority for the US intelligence agencies.

By Peter Martin and Katrina Manson



# Other motives

- **Publicity attacks**
- **Availability attacks**
  - Denial of Service (DoS), Distributed Denial of Service (DDoS)



# Threat Models

# Threat Models

- **Set of assumptions about the abilities of an adversary**
- **A way to identify & prioritize potential threats from an attacker's point of view**
  - Think about things that could go wrong
  - Bad guys don't follow rules: they don't care about your policies
  - We need to understand what types of attacks are possible
- **Assess**
  - What's valuable?
  - Where will you be likely to be attacked?
  - What are the most significant threats?
- **Think about entities in the system, how they communicate & store data**
  - Where are the trust boundaries?
  - Where and how is protection enforced?

# Trusted Computing Base and Supply Chain Vulnerabilities

# Trusted Computing Base (TCB)

**TCB = All hardware & software of a computing system critical to its security**

“The totality of protection mechanisms within it, including hardware, firmware, and software, the combination of which is responsible for enforcing a computer security policy.”

– Orange Book

*U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)*

**If the TCB is compromised, we can no longer guarantee the security of a system**

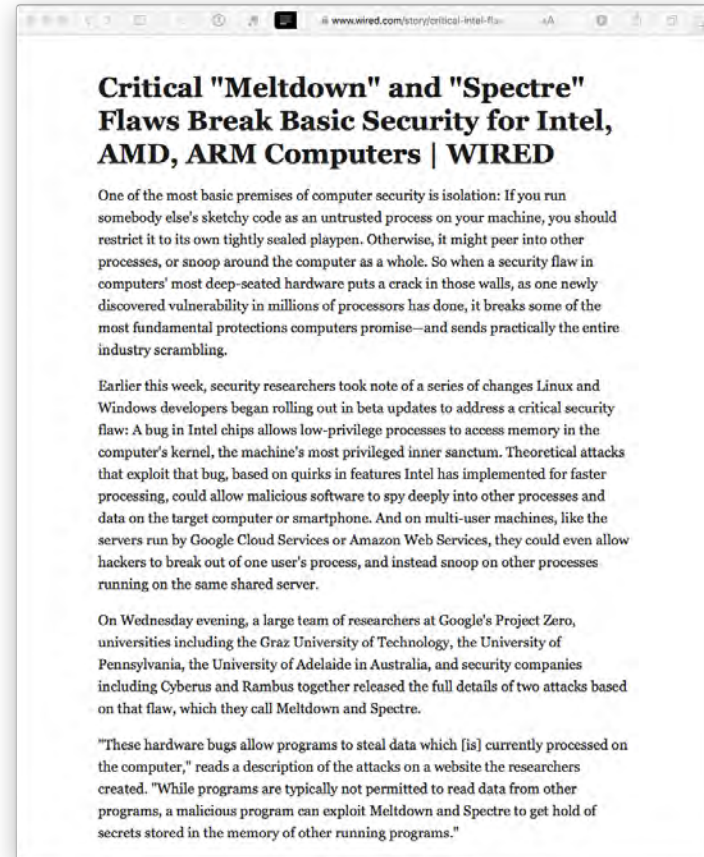
**Software that is part of the TCB must protect itself against tampering**

- Operating system memory protection is an example of this: an application may be compromised but the operating system is still intact and unaffected



# Jan 2018 – Meltdown & Spectre

- Intel chips do not have full memory protection when doing speculative execution
- **Vulnerability existed for 20 years!**
- **Meltdown**
  - Allows processes to access kernel memory
- **Spectre**
  - Allows processes to steal data from the memory of other processes
- **Also affects ARM & AMD CPUs**





# Rowhammer

- **Hardware-based attack discovered by Google Project Zero in 2014**
  - Exploits a weakness in modern DRAM chips.
- **Vulnerability**
  - Repeatedly accessing (or "hammering") a row of memory cells at high speeds can cause electrical interference that flips the bits in adjacent rows of memory cells
- **Attackers were able to**
  - **Corrupt sensitive data**, potentially crashing applications or the OS
  - **Gain escalated privileges** by modifying data such as page tables in the OS
  - **Bypass security mechanisms** to execute malicious code
- **Affects various operating systems and platforms**

The Trusted Computing Base includes all the hardware and software you depend on:

*Bootloaders, operating systems, compilers, utilities, libraries*

They're part of the supply chain that makes software and devices that run the software

# Supply chain attack hits Chrome extensions, could expose millions

Threat actor exploited phishing and OAuth abuse to inject malicious code

Connor Jones • Jan 22, 2025

Cybersecurity outfit Sekoia is warning Chrome users of a supply chain attack targeting browser extension developers that has potentially impacted hundreds of thousands of individuals already.

Dozens of Chrome extension developers have fallen victim to the attacks thus far, which aimed to lift API keys, session cookies, and other authentication tokens from websites such as ChatGPT and Facebook for Business.

## Chrome support impersonation

The attacker targeted dev teams with phishing emails seemingly from Chrome Web Store Developer Support, mimicking official communication, according to Yusoff and Sekoia.

The sample email, which appears in the report, shows the warnings that extensions may be pulled from Chrome over fake rule violations, such as unnecessary details in the extension's description.

Victims were lured into clicking a link disguised as an explanation of Chrome Web Store policies. The link led to a legitimate Google Accounts page, where they were prompted to approve access for a malicious OAuth app. Once developers granted the app permission, the attacker gained everything needed to upload compromised versions of their extensions to the Chrome Web Store.

[https://www.theregister.com/2025/01/22/supply\\_chain\\_attack\\_chrome\\_extension/](https://www.theregister.com/2025/01/22/supply_chain_attack_chrome_extension/)

# Popular NPM library hijacked to install password-stealers, miners

Lawrence Abrams • October 23, 2021

Hackers hijacked the popular **UA-Parser-JS** NPM library, with millions of downloads a week, to infect Linux and Windows devices with cryptominers and password-stealing trojans in a supply-chain attack.

The UA-Parser-JS library is used to parse a browser's user agent to identify a visitor's browser, engine, OS, CPU, and Device type/model.

The library is immensely popular, with millions of downloads a week and over 24 million downloads this month so far. In addition, the library is used in over a thousand other projects, including those by Facebook, Microsoft, Amazon, Instagram, Google, Slack, Mozilla, Discord, Elastic, Intuit, Reddit, and many more well-known companies.

...

On October 22<sup>nd</sup>, a threat actor published malicious versions of the UA-Parser-JS NPM library to install cryptominers and password-stealing trojans on Linux and Windows devices.

According to the developer, his NPM account was hijacked and used to deploy the three malicious versions of the library.

<https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/>

# Cisco's warning: Critical flaw in IOS routers allows 'complete system compromise'



Cisco has delivered updates to address four critical flaws affecting its industrial routers.

Liam Tung • June 4 2020

Cisco has disclosed four critical security flaws affecting router equipment that uses its IOS XE and IOS software.

The four critical flaws are part of Cisco's June 3 semi-annual advisory bundle for IOS XE and IOS networking software, which includes 23 advisories describing 25 vulnerabilities.

The 9.8 out of 10 severity bug, CVE-2020-3227, concerns the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software, which allows a remote attacker without credentials to execute Cisco IOx API commands without proper authorization.

IOx **mishandles requests for authorization tokens**, allowing an attacker to exploit the flaw with a specially crafted API call to request the token and then execute Cisco IOx API commands on the device, according Cisco.

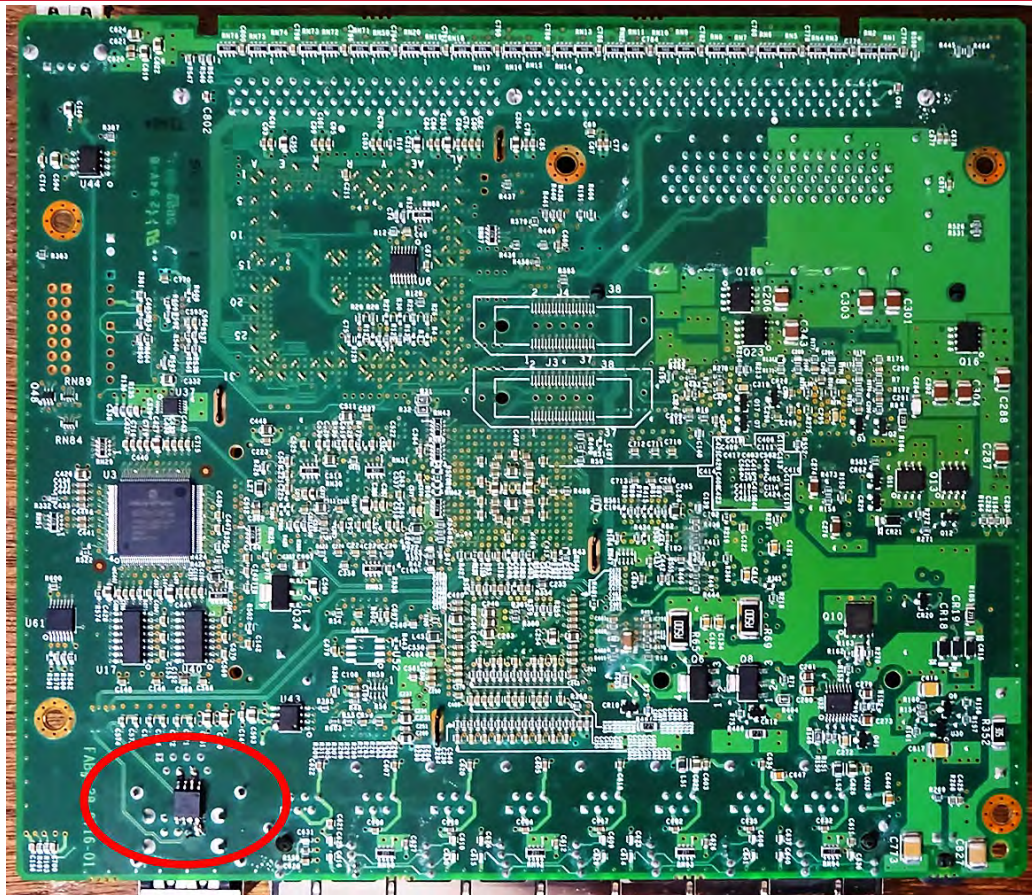
<https://www.zdnet.com/article/ciscos-warning-critical-flaw-in-ios-routers-allows-complete-system-compromise/>

# Attacks on 3<sup>rd</sup> party software, services, hosting sites

- **June 2024: CDK Global ransomware attack – 15,000 auto dealerships**
  - Backend system used by car dealers
  - Crippled operations of 15,000 auto dealerships across the U.S. & Canada
- **July 2024: Snowflake data breach – 100s of millions of AT&T records**
  - Attackers downloaded hundreds of millions of phone call and text message records of AT&T customers
  - AT&T uses Snowflake for data warehousing & analytics
  - Attackers used stolen credentials to log in
- **July 2024: CrowdStrike bug – 8.5 million Windows servers worldwide**
  - CrowdStrike provides endpoint protection software
  - Not an attack! A buggy update (NULL pointer dereference) caused the program to crash
  - Largest IT outage in history: 8.5 millions servers affected (auto, healthcare, aviation, broadcasting, banking)
  - More than 6,700 flights were canceled as a result

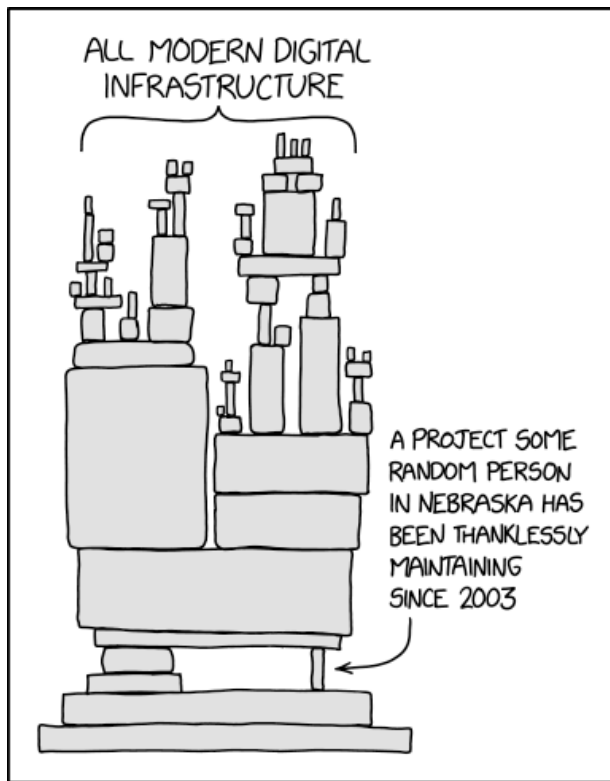
# Do you trust the entire supply chain?

- Alter the circuit design
- Add components after the fact
- Modify the CPU
- Modify the bootloader, firmware, or pre-installed software
- Add malware to the compiler used to build the software
- Add malware to libraries used by the apps



# Supply chain problems

- Do you trust the hardware?
- Do you trust every piece of code that is required to run your infrastructure?
- Do you know where it comes from?
- How actively it's maintained?
- Whether it's been audited for vulnerabilities?



<https://xkcd.com/2347/>





[Home](#) » [News & Events](#) » [Blogs](#) » [Tech@FTC](#) » [FTC warns companies to remediate Log4j security vulnerability](#)

## FTC warns companies to remediate Log4j security vulnerability

By: This blog is a collaboration between CTO and DPIP staff and the AI Strategy team | Jan 4, 2022 9:19AM

SHARE THIS PAGE



**TAGS:** [Accountability](#) | [Data security](#) | [Patches](#)

Log4j is a ubiquitous piece of software used to record activities in a wide range of systems found in consumer-facing products and services. Recently, a serious vulnerability in the popular Java logging package, Log4j (CVE-2021-44228) was disclosed, posing a severe risk to millions of consumer products to enterprise software and web applications. This vulnerability is being widely exploited by a growing set of attackers.

When vulnerabilities are discovered and exploited, it risks a loss or breach of personal information, financial loss, and other irreversible harms. The duty to take reasonable steps to mitigate known software vulnerabilities

### Subscribe

[Subscribe to Tech@FTC Blog updates](#)

### Upcoming FTC Tech Events

Currently we have no upcoming Tech events. Please check back soon.

### Additional Information

[Office of Technology Research & Investigation](#)

<https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability>

- **XZ Utils:** set of open-source software for compression and decompression
- **Included with many Linux distributions & widely used**
- **Around 2021:**
  - A developer with the name Jia Tan started to make requests for bug fixes and improvements
  - Jia built trust and eventually got permission to commit and then be a release manager
  - **Social engineering:** Fake accounts created for sending lots of bug & feature requests pressured the original maintainer into adding Jia Tan as another maintainer
- **In 2023:**
  - After two years of fixing bugs, Jia Tan introduced a few changes to XZ. Among these changes was a sophisticated backdoor.
  - This would enable an attacker to run arbitrary commands on software that used XZ Utils, like ssh, the secure shell
  - It almost made it to every major Linux distribution
- **But in March 2024:**
  - A Microsoft employee, Andres Freund, discovered an unexpected 500 ms latency after doing an update
  - He traced it to this unexpected code in XZ Utils.

# New UEFI vulnerabilities send firmware devs industry wide scrambling

The ability to attack the boot process

PixieFail is a huge deal for cloud and data centers. For the rest, less so. 

Dan Goodin • January 17, 2024

UEFI firmware from five of the leading suppliers contains vulnerabilities that allow attackers with a toehold in a user's network to infect connected devices with malware that runs at the firmware level.

The vulnerabilities, which collectively have been dubbed PixieFail by the researchers who discovered them, pose a threat mostly to public and private data centers and possibly other enterprise settings. People with even minimal access to such a network—say a paying customer, a low-level employee, or an attacker who has already gained limited entry—can exploit the vulnerabilities to infect connected devices with a malicious UEFI.

Short for Unified Extensible Firmware Interface, UEFI is the low-level and complex chain of firmware responsible for booting up virtually every modern computer. By installing malicious firmware that runs prior to the loading of a main OS, UEFI infections can't be detected or removed using standard endpoint protections. They also give unusually broad control of the infected device.

...

The implementation is incorporated into offerings from Arm Ltd., Insyde, AMI, Phoenix Technologies, and Microsoft.

<https://arstechnica.com/security/2024/01/new-uefi-vulnerabilities-send-firmware-devs-across-an-entire-ecosystem-scrambling/>

# Malicious Chinese SDK In 1,200 iOS Apps With Billions Of Installs Causing ‘Major Privacy Concerns To Hundreds Of Millions Of Consumers’

Unknowingly bundling spyware into an app

John Koetsier • August 24, 2020

Forbes

A Chinese ad network named Mintegral is accused of spying on user activity and committing ad fraud in more than 1,200 apps with 300 million installs per month since July 2019. Mintegral is headquartered in Beijing, China, and is owned by another Chinese ad network, Mobvista, which has a head office in Guangzhou, China.

One of the apps, Helix Jump, has over 500 million total installs. Other popular apps that are impacted include Talking Tom, PicsArt, Subway Surfers and Gardenscapes.

All together, this likely impacts billions of total app installs on iPhone and iPad.

There’s no exact number on how many devices or iPhone users are impacted, but Snyk says this is a “major privacy concern to hundreds of millions of consumers.”

<https://johnkoetsier.com/malicious-chinese-sdk-in-1200-ios-apps-with-billions-of-installs-causing-major-privacy-concerns-to-hundreds-of-millions-of-consumers/>

# Pre-installed malware

ars TECHNICA

NO FREE LUNCH —

## US Government-funded Android phones come preinstalled with unremovable malware

Phones were sold to low-income people under the FCC's Lifeline Assistance program.

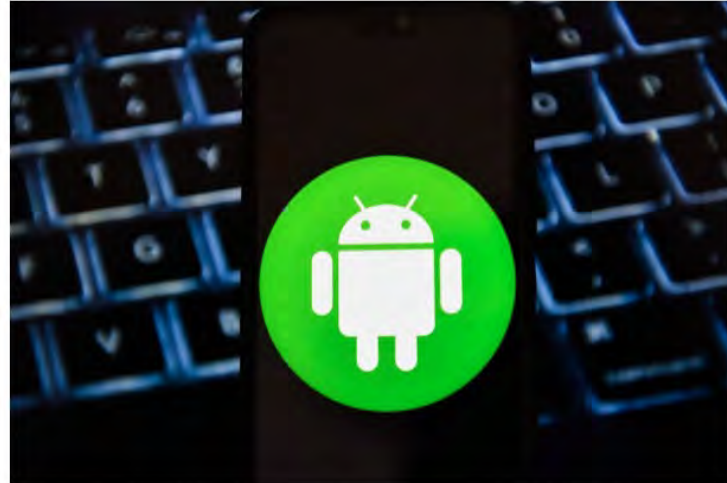
DAN GOODIN - 1/9/2020, 4:26 PM

## Android malware that comes preinstalled is a massive threat

The Android Security team's former tech lead, who's now a security researcher on Google's Project Zero, breaks down why.



Alfred Ng · Aug. 8, 2019 2:30 p.m. PT



When malware comes preinstalled on Android devices, it's much harder to remove, Google's researchers said.

Omar Marques/SOPA Images/LightRocket via Getty Images

c|net

# Millions of Android phones come with pre-installed malware, and there's no easy fix

Affordable phones are nice, but that doesn't mean they should be riddled with malicious code

Adrian Potoroaca • May 12, 2023

Researchers at Trend Micro are sounding the alarm about the growing trend of Android devices that come with malicious software pre-installed. While you can easily remove an app you've downloaded from the Play Store, addressing malware embedded in system apps or device firmware is a significantly more challenging task.

Senior Trend Micro researcher Fyodor Yarochkin says pre-installed malware has become much more common in recent years, partly due to a race to the bottom among mobile firmware developers. Once selling firmware became unprofitable, many developers began offering it for free.

As expected, there's a catch to this new business model – many of the firmware images analyzed by Trend Micro contained bits of code described as "silent plugins." The researchers have discovered over 80 flavors so far, but only a few have seen widespread distribution. The more popular ones are being sold underground and promoted on Facebook, YouTube, and various blogs.

<https://www.techspot.com/news/98667-millions-android-phones-come-pre-installed-malware-there.html>

# Don't underestimate the human element

## Humans are

- Bad at storing keys
- Poor at estimating risk
- Not accurate
- Careless
- Gullible



<https://xkcd.com/1777/>

## Social engineering is the top threat

hacking / CORY DOCTOROW / 11:44 AM FRI

**It turns out that halfway clever phishing attacks really, really work**

One account. All of Google.

Sign in to continue to Gmail

Enter your email

Next

Need help?

A new phishing attack hops from one Gmail account to the next by searching through compromised users' previous emails for messages with attachments, then replies them from the compromised account, replacing the link to the attachment with a lookalike that sends you to a fake Google login page (they use some trickery to hide the fake in the location bar); the attackers stand by and if you enter your login/pass, they immediately seize control of your account and attack your friends.

# The End